

COMP

Alex J. De Castroverde

Nevada Bar No. 6950

Ryan Samano

Nevada Bar No. 15995

DE CASTROVERDE LAW GROUP

1149 S. Maryland Pkwy

Las Vegas, NV 89104

Tel: 702.222.9999

Fax: 702.383.8741

Email: ryan@dlgteam.com

Attorneys for Plaintiff

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

ROBERT DAPELLO and JONATHAN FARNAM
on behalf of themselves and all others similarly
situated,

Plaintiffs,

vs.

RIVERSIDE RESORT & CASINO, INC. and
RIVERSIDE RESORT & CASINO, LLC

Defendants.

Case No.:

COMPLAINT-CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiffs Robert Dapello and Jonathan Farnam (collectively “Plaintiffs”) bring this Class Action Complaint against Riverside Resort & Casino, Inc. and Riverside Resort & Casino, LLC (“Riverside” or “Defendants”), individually and on behalf of all others similarly situated (“Class Members”), and allege, upon personal knowledge as to their own actions and their counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information (“PII”)¹ of at least 55,150 individuals,² including,

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79..

1 on information and belief such personal information an employer keeps for their employees, such
2 as name, date of birth, federal/state identification numbers, social security number, financial
3 information and/or other information such as phone number, address, and email address.

4 2. Riverside is a resort and casino located in Laughlin, Nevada that consists of a
5 hotel, an RV park, eight restaurants, entertainment venues and other facilities. Approximately five
6 million people visit the resort each year and it employs more than 1,719 people and generates \$316
7 million in annual revenue.³

8 3. Prior to and through July 25, 2024, Defendant obtained the PII of Plaintiffs and
9 Class Members, including by collecting it directly from Plaintiffs and Class Members.

10 4. On information and belief prior to and through July 25, 2024, Defendant stored
11 the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment on
12 Defendant's network.⁴

13 5. Although Defendant's notice is unclear, at some point on or before July 25, 2024,
14 Defendant allowed cybercriminals unfettered access to Plaintiffs' and the Class Members' highly
15 sensitive information.

16 6. Defendant determined that, during the Data Breach, cybercriminals accessed
17 and/or acquired the PII of Plaintiffs and Class Members. On information and belief, a ransomware
18 gang has claimed responsibility for the attack and has threatened to release the PII to the public.⁵

19 7. On or around September 5, 2024, Defendant began notifying the approximately
20 55,155 people affected, including Plaintiffs and Class Members, of the Data Breach.⁶ A sample of
21 the breach notice is attached hereto as Exhibit A.

22
23
24
25
26 ²<https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ab5c465c-1b23-4a88-9a62-253cad91b22b.html> (last viewed September 12, 2024).

27 ³ <https://www.jdsupra.com/legalnews/riverside-resort-casino-notifies-5193196/> (last viewed September 12, 2024).

28 ⁴ *Id.*

⁵ <https://www.jdsupra.com/legalnews/riverside-resort-casino-notifies-5193196/> (last viewed September 12, 2024).

⁶ https://www.mohavedailynews.com/news/over-55-000-affected-in-riverside-resort-casino-data-breach/article_e2d3f2ca-709d-11ef-9c9c-db226fb385f6.html (last viewed September 12, 2024)

1 8. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs
2 and Class Members, Defendant assumed legal and equitable duties to those individuals to protect
3 and safeguard that information from unauthorized access and intrusion. Defendant admits that the
4 unencrypted PII that was accessed and/or acquired by an unauthorized actor.

5 9. The exposed PII of Plaintiffs and Class Members can be sold on the dark web.
6 Hackers can access and then offer for sale the un-encrypted, unredacted PII to criminals. Plaintiffs
7 and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the
8 loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive
9 information.

10 10. The PII was compromised due to Defendant's negligent and/or careless acts and
11 omissions and the failure to protect the PII of Plaintiffs and Class Members. Defendant has also
12 purposefully maintained secret the specific vulnerabilities and root causes of the breach and has
13 not informed Plaintiffs and Class Members of that information.

14 11. Prior to receiving notification, Plaintiffs and Class Members had no idea their PII
15 had been compromised, and that they were, and continue to be, at significant risk of identity theft
16 and various other forms of personal, social, and financial harm, including the sharing and
17 detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

18 12. Plaintiffs bring this action on behalf of all persons whose PII was compromised as
19 a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members;
20 (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices;
21 and (iii) effectively secure hardware containing protected PII using reasonable and effective
22 security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to
23 negligence and violates federal and state statutes.

24 13. Plaintiffs and Class Members have suffered injuries as a result of Defendant's
25 conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses
26
27
28

1 associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or
2 unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the
3 actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure
4 of their private information, and (v) the continued and certainly increased risk to their PII, which:
5 (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b)
6 may remain backed up in Defendant's possession and is subject to further unauthorized disclosures
7 so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.
8

9 14. Defendant disregarded the rights of Plaintiffs and Class Members by
10 intentionally, willfully, recklessly, or negligently failing to take and implement adequate and
11 reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded,
12 failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow
13 applicable, required and appropriate protocols, policies and procedures regarding the encryption of
14 data, even for internal use. As a result, the PII of Plaintiffs and Class Members were compromised
15 through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing
16 interest in ensuring that their information is and remains safe, and they should be entitled to
17 injunctive and other equitable relief.
18

19 15. On behalf of themselves and the Class as defined herein, Plaintiffs bring claims
20 for negligence, breach of fiduciary duty, breach of confidence, breach of express contract, breach
21 of implied contract, and, in the alternative to their contract-based claims, unjust enrichment. The
22 remedies Plaintiffs seek include actual, nominal, and putative damages; appropriate injunctive and
23 declaratory relief; and attorneys' fees, costs, and expenses.
24

25 II. PARTIES

26 16. Plaintiff Robert Dapello is now and has at all relevant times been a resident and
27 citizen of Arizona, currently residing in Bullhead City, Arizona.
28

17. Plaintiff Jonathan Farnam is now and has at all relevant times been a resident and

1 citizen of Arizona, currently residing in Fort Mohave, Arizona.

2 18. Defendant Riverside Resort and Casino, Inc. is a Nevada domestic corporation
3 with a principal place of business in Laughlin, Nevada. Defendant may be served by serving its
4 registered agent, Sierra Corporate Services- Las Vegas, 2300 West Sahara Ave. Ste. 1200, Las
5 Vegas, Nevada 89102.

6 19. Defendant Riverside Resort and Casino, LLC is a Nevada limited liability
7 company with a principal place of business in Laughlin, Nevada. Defendant may be served by
8 serving its registered agent, Sierra Corporate Services- Las Vegas, 2300 West Sahara Ave. Ste.
9 1200, Las Vegas, Nevada 89102.

10 20. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its
11 owners, predecessors, successors, subsidiaries, agents and/or assigns.

12 **III. JURISDICTION AND VENUE**

13 21. This Court has subject matter and diversity jurisdiction over this action under 28
14 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum
15 or value of \$5 million, exclusive of interest and costs, there are at least 55,155 members in the
16 proposed class, and at least one Class Member (both Plaintiffs) is a citizen of a state different from
17 Defendant to establish minimal diversity.

18 22. Defendant Riverside Resort and Casino, Inc. is a citizen of Nevada because it is a
19 corporation formed under Nevada law with its principal place of business in Laughlin, Nevada.

20 23. Defendant Riverside Resort and Casino, LLC is a citizen of Nevada because it is
21 a corporation formed under Nevada law with its sole manager's residence in Laughlin, Nevada.

22 24. The District of Nevada has personal jurisdiction over Defendant because it
23 conducts substantial business in Nevada and this District and the location of the corporate
24 headquarters that collected and/or stored the PII of Plaintiff and Class Members in this District.

25 25. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant

operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

26. Defendant collected the PII of Plaintiffs and Class Members and stored it, unencrypted, on Defendant's internet-accessible network.

27. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

28. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

29. On or about September 5, 2024, Defendant sent Plaintiffs and Class Members a *Notice of Data Breach* informing Plaintiffs and other Class Members that:

Riverside Resort & Casino (Riverside) is writing to inform you of a recent data security incident...

What Happened

On July 25, 2024, Riverside learned of suspicious activity in its environment. ..Through this investigation, Riverside determined that an unauthorized third party potentially accessed and acquired certain files during this incident. Riverside then performed an extensive and comprehensive review of the data to identify what personal information may have been impacted in this incident.

On August 9, 2024, Riverside identified the persons whose sensitive information was potentially impacted.

...

What Information Was Involved?

1 The following data may have been subject to unauthorized access and acquisition:
2 Name and Social Security number.

3 30. Defendant admitted in the *Notice of Data Breach* that an unauthorized actor
4 accessed sensitive information about Plaintiffs and Class Members.

5 31. The details of the root cause of the Data Breach, the vulnerabilities exploited, and
6 the remedial measures undertaken to ensure a breach does not occur again have not been shared
7 with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their
8 information remains protected.

9 32. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the
10 dark web, or simply fall into the hands of companies that will use the detailed PII for targeted
11 marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can
12 easily access the PII of Plaintiffs and Class Members.

13 33. Defendant did not use reasonable security procedures and practices appropriate to
14 the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class
15 Members, causing the exposure of PII for Plaintiffs and Class Members.

16 34. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII,
17 Defendant should have accessed readily available and accessible information about potential
18 threats for the unauthorized exfiltration and misuse of such information.

19 35. In the years immediately preceding the Data Breach, Defendant knew or should
20 have known that Defendant's computer systems were a target for cybersecurity attacks because
21 warnings were readily available and accessible via the internet.

22 36. In tandem with the increase in data breaches, the rate of identity theft complaints
23 has also increased over the past few years. For instance, in 2017, 2.9 million people reported some
24
25
26
27
28

1 form of identity fraud compared to 5.7 million people in 2021.⁷

2 37. The type and breadth of data compromised in the Data Breach makes the
3 information particularly valuable to thieves and leaves Defendant's customers especially
4 vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

5 38. Private Information is a valuable property right.⁸ The value of Private Information
6 as a commodity is measurable.⁹ "Firms are now able to attain significant market valuations by
7 employing business models predicated on the successful use of personal data within the existing
8 legal and regulatory frameworks."¹⁰ American companies are estimated to have spent over \$19
9 billion on acquiring personal data of consumers in 2018.¹¹ It is so valuable to identity thieves that
10 once Private Information has been disclosed, criminals often trade it on the "cyber black-market,"
11 or the "dark web," for years afterwards.

12 39. As a result of their real value and the recent large-scale data breaches, identity
13 thieves and cyber criminals have openly posted credit card numbers, Social Security numbers,
14 Private Information, and other sensitive information directly on various internet websites, making
15 the information publicly available. This information from various breaches, including the
16 information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves
17 and more damaging to victims.

21 ⁷ Facts + Statistics: Identity Theft and Cybercrime, INSURANCE INFORMATION INSTITUTE,
22 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-andcybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20> (last visited Apr. 27, 2023).

23 ⁸ See Marc Van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFORMATION &
24 COMMUNICATION TECHNOLOGY 26 (May 2015),

25 https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal]
26 information is well understood by marketers who try to collect as much data about personal conducts and preferences
27 as possible . . .").

⁹ Robert Lowes, Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market, MEDSCAPE
(Apr. 28, 2014), <http://www.medscape.com/viewarticle/824192>.

¹⁰ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD
(Apr. 2, 2013),

https://www.oecd-ilibrary.org/science-andtechnology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

¹¹ U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5%
28 from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018),
<https://www.iab.com/news/2018-state-of-data-report/>.

1 40. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in
2 1,000+ SEC filings over the past year,” that “[r]ansomware gangs are now ferociously aggressive
3 in their pursuit of big companies. They breach networks, use specialized tools to maximize
4 damage, leak corporate information on dark web portals, and even tip journalists to generate
5 negative news for companies as revenge against those who refuse to pay.”¹²

6
7 41. In September 2020, the United States Cybersecurity and Infrastructure Security
8 Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted
9 their ransomware tactics over time to include pressuring victims for payment by threatening to
10 release stolen data if they refuse to pay and publicly naming and shaming victims as secondary
11 forms of extortion.”¹³

12 42. According to the U.S. Government Accountability Office, which conducted a
13 study regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more
14 before being used to commit identity theft. Further, once stolen data has been sold or posted on the
15 [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that
16 attempt to measure the harm resulting from data breaches cannot necessarily rule out all future
17 harm.”

18
19 43. That is because any victim of a data breach is exposed to serious ramifications
20 regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable
21 information is to monetize it. They do this by selling the spoils of their cyberattacks on the black
22 market to identity thieves who desire to extort and harass victims, and to take over victims’
23 identities to engage in illegal financial transactions under the victims’ names. Because a person’s
24 identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a
25
26

27
28 ¹² ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added),
available at <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last
visited Feb. 24, 2023).

1 person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the
2 victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking
3 technique referred to as "social engineering" to obtain even more information about a victim's
4 identity, such as a person's login credentials or Social Security number. Social engineering is a
5 form of hacking whereby a data thief uses previously acquired information to manipulate
6 individuals into disclosing additional confidential or personal information through means such as
7 spam phone calls and text messages or phishing emails.
8

9 44. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to
10 exhaust financial accounts, receive medical treatment, open new utility accounts, and incur
11 charges and credit in a person's name.

12 45. The FTC recommends that identity theft victims take several steps to protect their
13 personal and financial information after a data breach, including contacting one of the credit
14 bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if
15 someone steals their identity), reviewing their credit reports, contacting companies to remove
16 fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit
17 reports.
18

19 46. Identity thieves use stolen personal information such as Social Security numbers
20 for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.
21 According to Experian, one of the largest credit reporting companies in the world, "[t]he research
22 shows that personal information is valuable to identity thieves, and if they can get access to it, they
23 will use it" to among other things: open a new credit card or loan, change a billing address so the
24 victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and
25 write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID,
26
27

28 ¹³ U.S. CISA, Ransomware Guide–September 2020, available at
<https://www.cisa.gov/stopransomware/ransomware-guide> (last visited April 21, 2023).

1 and/or use the victim's information in the event of arrest or court action.

2 47. Identity thieves can also use the victim's name and Social Security number to
3 obtain government benefits; or file a fraudulent tax return using the victim's information. In
4 addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent
5 a house or receive medical services in the victim's name.

6 48. Even if stolen PII does not include financial or payment card account information,
7 that does not mean there has been no harm, or that the breach does not cause a substantial risk of
8 identity theft. Freshly stolen information can be used with success against victims in specifically
9 targeted efforts to commit identity theft known as social engineering or spear phishing. In these
10 forms of attack, the criminal uses the previously obtained PII about the individual, such as name,
11 address, email address, and affiliations, to gain trust and increase the likelihood that a victim will
12 be deceived into providing the criminal with additional information.

13 49. Consumers place a high value on the privacy of that data. Researchers shed light
14 on how much consumers value their data privacy—and the amount is considerable. Indeed, studies
15 confirm that “when privacy information is made more salient and accessible, some consumers are
16 willing to pay a premium to purchase from privacy protective websites.”¹⁴

17 50. This readily available and accessible information confirms that, prior to the Data
18 Breach, Defendant knew or should have known that (i) cybercriminals were targeting big
19 companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of
20 big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark
21 web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

22 51. In light of the information readily available and accessible on the internet before
23 the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class
24

Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

52. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

53. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

54. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members.

55. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

56. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

57. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."¹⁵

58. To prevent and detect ransomware attacks, including the ransomware attack that

¹⁴ Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), <https://www.guanotronic.com/~serge/papers/isr10.pdf>.

¹⁵ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Feb. 24, 2023).

1 resulted in the Data Breach, Defendant could and should have implemented, as recommended by
2 the United States Government, the following measures:

3 a. Implement an awareness and training program. Because end users are
4 targets, employees and individuals should be aware of the threat of ransomware and how it
5 is delivered.

6 b. Enable strong spam filters to prevent phishing emails from reaching the end
7 users and authenticate inbound email using technologies like Sender Policy Framework
8 (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and
9 DomainKeys Identified Mail (DKIM) to prevent email spoofing.

10 c. Scan all incoming and outgoing emails to detect threats and filter
11 executable files from reaching end users.

12 d. Configure firewalls to block access to known malicious IP addresses.

13 e. Patch operating systems, software, and firmware on devices. Consider
14 using a centralized patch management system.

15 f. Set anti-virus and anti-malware programs to conduct regular scans
16 automatically.

17 g. Manage the use of privileged accounts based on the principle of least
18 privilege: no users should be assigned administrative access unless absolutely needed; and
19 those with a need for administrator accounts should only use them when necessary.

20 h. Configure access controls—including file, directory, and network share
21 permissions—with least privilege in mind. If a user only needs to read specific files, the
22 user should not have write access to those files, directories, or shares.

23 i. Disable macro scripts from office files transmitted via email. Consider
24 using Office Viewer software to open Microsoft Office files transmitted via email instead
25 of full office suite applications. Implement Software Restriction Policies (SRP) or other
26
27
28

controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

j. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

k. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

l. Execute operating system environments or specific programs in a virtualized environment.

m. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁶

59. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication]

¹⁶ *Id.* at 3-4.

and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁷

60. Given that Defendant was storing the PII of thousands individuals, Defendant could and should have implemented all the above measures to prevent and detect ransomware attacks.

61. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of thousands of individuals, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

62. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

63. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is

exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

64. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

65. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁸ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁹

66. The ramifications of Defendant’s failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

67. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁰ Experian reports that a stolen credit

¹⁷ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Feb. 24, 2023).

¹⁸ 17 C.F.R. § 248.201 (2013).

¹⁹ *Id.*

²⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Feb. 24, 2023).

or debit card number can sell for \$5 to \$110 on the dark web.²¹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²²

68. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²³

70. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

71. The fraudulent activity resulting from the Data Breach may not come to light for years.

72. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

²¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 24, 2023).

²² *In the Dark*, VPN Overview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Feb. 24, 2023).

²³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Feb. 24, 2023).

1 from data breaches cannot necessarily rule out all future harm.²⁴

2 73. At all relevant times, Defendant knew, or reasonably should have known, of the
3 importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security
4 numbers, and of the foreseeable consequences that would occur if Defendant's data security
5 system was breached, including, specifically, the significant costs that would be imposed on
6 Plaintiff and Class Members as a result of a breach.
7

8 74. Plaintiffs and Class Members now face years of constant surveillance of their
9 financial and personal records, monitoring, and loss of rights. The Classes are incurring and will
10 continue to incur such damages in addition to any fraudulent use of their PII.

11 75. Defendant was, or should have been, fully aware of the unique type and the
12 significant volume of data contained in Defendant's contract search tool, amounting to potentially
13 tens of thousands of individuals detailed, personal information and, thus, the significant number of
14 individuals who would be harmed by the exposure of the unencrypted data.
15

16 76. To date, Defendant has offered Plaintiffs and Class Members 12 months of
17 complimentary credit monitoring and identify protection services through Single Bureau Credit
18 Monitoring/Single Bureau Credit Report/Single Bureau Credit Score Services. The offered service
19 is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come,
20 particularly in light of the PII at issue here.
21

22 77. The injuries to Plaintiffs and Class Members were directly and proximately
23 caused by Defendant's failure to implement or maintain adequate data security measures for the
24 PII of Plaintiffs and Class Members.

25 ***Plaintiffs' Experiences***
26
27

28 ²⁴ Report to Congressional Requesters, GAO, at 29 (June 2007), available at:
<https://www.gao.gov/assets/gao-07-737.pdf> (last visited Feb. 24, 2023).

1 78. Plaintiffs received notice from Defendant that their personal information kept by
2 Defendant had been compromised as a result of the Data Breach.

3 79. As a result of the Data Breach, Plaintiffs' sensitive information was accessed
4 and/or acquired by an unauthorized actor. The confidentiality of Plaintiffs' sensitive information
5 has been irreparably harmed. For the rest of their lives, Plaintiffs will have to worry about when
6 and how their sensitive information may be shared or used to their detriment.

7
8 80. As a result of the Data Breach notice, Plaintiffs spent time dealing with the
9 consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice*
10 *of Data Breach* and self-monitoring their accounts. This time has been lost forever and cannot be
11 recaptured.

12 81. Additionally, Plaintiffs are very careful about sharing their sensitive PII. They
13 have never knowingly transmitted unencrypted sensitive PII over the internet or any other
14 unsecured source.

15
16 82. Plaintiffs store any documents containing their sensitive PII in a safe and secure
17 location or destroys the documents. Moreover, they diligently choose unique usernames and
18 passwords for their various online accounts.

19 83. Defendant's data security shortcomings resulted in the Data Breach and caused
20 Plaintiffs significant injuries and harm in several ways. For example, Plaintiffs have devoted and
21 will continue to devote significant time, energy, and money to: closely monitoring their bills,
22 records, and credit and financial accounts; changing login and password information on any
23 sensitive account; carefully screening and scrutinizing phone calls, emails, and other
24 communications to ensure that they are not being targeted by identity theft scams, medical identity
25 theft scams, or other attempts at fraud; searching for suitable identity theft protection and credit
26 monitoring services and paying for such services to protect themselves; and placing fraud alerts
27 and/or credit freezes on their credit file. Plaintiffs have taken or will be forced to take these
28

measures to mitigate their potential damages because of the Data Breach.

84. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, especially their Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

85. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

86. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure and Local Rule 23.1.

87. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All persons in the United States and its territories whose PII was compromised in the Data Breach, including all individuals who received a data breach notification letter from Defendant. (the "Nationwide Class").

88. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

89. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

90. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of

all members is impracticable. Defendant reported that 55,150 were impacted in the Data Breach, and the Classes are apparently identifiable within Defendant's records.²⁵

91. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether Defendant's actions and its allegedly lax data security practices used to protect Plaintiffs' and Class Members' PII violated the FTC Act and/or other state laws and/or Defendant's other duties alleged herein;

c. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

e. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

f. Whether an implied contract existed between Class Members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

²⁵

<https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ab5c465c-1b23-4a88-9a62->

1 g. Whether an express contract existed between class members and Defendant
2 providing that Defendant would implement and maintain reasonable security measures to
3 protect and secure Class Members' PII from unauthorized access and disclosure;

4 h. Whether Plaintiffs and Class Members are intended third party
5 beneficiaries of contracts between Defendant and third parties, and if so whether
6 Defendant breached those contracts;

7 i. Whether injunctive relief is appropriate and, if so, what injunctive relief is
8 necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class
9 Members;

10 j. Whether Defendant's actions and inactions alleged herein constitute gross
11 negligence;

12 k. Whether Defendant breached its duties to protect Plaintiffs and Class
13 Members' Private Information; and

14 l. Whether Plaintiffs and all other members of the Class are entitled to
15 damages and the measure of such damages and relief.

16 92. Defendant engaged in a common course of conduct giving rise to the legal rights
17 sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members.
18 Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous
19 common questions that dominate this action.

20 93. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other
21 Class Members because all had their PII compromised as a result of the Data Breach, due to
22 Defendant's misfeasance.

23 94. Policies Generally Applicable to the Classes: This class action is also appropriate
24 for certification because Defendant has acted or refused to act on grounds generally applicable to
25 Class Members.

1 the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible
2 standards of conduct toward Class Members and making final injunctive relief appropriate with
3 respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class
4 Members uniformly and Plaintiffs challenge of these policies hinges on Defendant's conduct with
5 respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.
6

7 95. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent
8 and protect the interests of Class Members in that they have no disabling conflicts of interest that
9 would be antagonistic to those of the other Members of the Classes. Plaintiffs received the
10 notification of the data breach and have experienced actual damages as a result of the breach.
11 Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the
12 infringement of the rights and the damages they have suffered are typical of other Class Members.
13 Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs
14 intend to prosecute this action vigorously.
15

16 96. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an
17 appropriate method for fair and efficient adjudication of the claims involved. Class action
18 treatment is superior to all other available methods for the fair and efficient adjudication of the
19 controversy alleged herein; it will permit a large number of Class Members to prosecute their
20 common claims in a single forum simultaneously, efficiently, and without the unnecessary
21 duplication of evidence, effort, and expense that hundreds of individual actions would require.
22 Class action treatment will permit the adjudication of relatively modest claims by certain Class
23 Members, who could not individually afford to litigate a complex claim against large corporations,
24 like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it
25 would still be economically impractical and impose a burden on the courts.
26

27 97. The nature of this action and the nature of laws available to Plaintiffs and Class
28 Members make the use of the class action device a particularly efficient and appropriate procedure

1 to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would
2 necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the
3 limited resources of each individual Class Member with superior financial and legal resources; the
4 costs of individual suits could unreasonably consume the amounts that would be recovered; proof
5 of a common course of conduct to which Plaintiffs were exposed is representative of that
6 experienced by the Classes and will establish the right of each Class Member to recover on the
7 cause of action alleged; and individual actions would create a risk of inconsistent results and would
8 be unnecessary and duplicative of this litigation.
9

10 98. The litigation of the claims brought herein is manageable. Defendant's uniform
11 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
12 Members demonstrate that there would be no significant manageability problems with prosecuting
13 this lawsuit as a class action.
14

15 99. Adequate notice can be given to Class Members directly using information
16 maintained in Defendant's records.

17 100. Finally, all members of the proposed Class are readily ascertainable. Defendant
18 has access to class members' names and addresses affected by the Data Breach. Indeed, class
19 members have already been preliminarily identified and sent notice of the Data Breach.
20

21 101. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
22 properly secure the PII of Class Members, Defendant may continue to refuse to provide proper
23 notification to Class Members regarding the Data Breach, and Defendant may continue to act
24 unlawfully as set forth in this Complaint.

25 102. Further, Defendant has acted or refused to act on grounds generally applicable to
26 the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to
27 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil
28 Procedure.

1 103. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification
2 because such claims present only particular, common issues, the resolution of which would
3 advance the disposition of this matter and the parties' interests therein. Such particular issues
4 include, but are not limited to:

5 a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to
6 exercise due care in collecting, storing, using, and safeguarding their PII;

7 b. Whether Defendant breached a legal duty to Plaintiffs and Class Members
8 to exercise due care in collecting, storing, using, and safeguarding their PII;

9 c. Whether Defendant failed to comply with its own policies and applicable
10 laws, regulations, and industry standards relating to data security;

11 d. Whether an implied contract existed between Defendant on the one hand,
12 and Plaintiffs and Class Members on the other, and the terms of that implied contract;

13 e. Whether Defendant breached the implied contract;

14 f. Whether Defendant adequately and accurately informed Plaintiffs and Class
15 Members that their PII had been compromised;

16 g. Whether Defendant failed to implement and maintain reasonable security
17 procedures and practices appropriate to the nature and scope of the information
18 compromised in the Data Breach;

19 h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by
20 failing to safeguard the PII of Plaintiffs and Class Members; and,

21 i. Whether Class Members are entitled to actual, consequential, and/or
22 nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.
23
24
25

26
27 **COUNT I**
28 **NEGLIGENCE**
 (On Behalf of Plaintiff and the Classes)

1 104. Plaintiffs and the Class reallege and incorporate by reference herein all the
2 preceding allegations above as if fully alleged herein.
3

4 105. Defendant has full knowledge of the sensitivity of the PII and the types of harm
5 that Plaintiff and the Classes could and would suffer if the PII were wrongfully disclosed.

6 106. Defendant knew or reasonably should have known that the failure to exercise due
7 care in the collecting, storing, and using of the PII of Plaintiffs and the Classes involved an
8 unreasonable risk of harm to Plaintiffs and the Classes, even if the harm occurred through the
9 criminal acts of a third party.
10

11 107. Defendant had a duty to exercise reasonable care in safeguarding, securing, and
12 protecting such information from being compromised, lost, stolen, misused, and/or disclosed to
13 unauthorized parties. This duty includes, among other things, designing, maintaining, and testing
14 Defendant's security protocols to ensure that the PII of Plaintiffs and the Classes in Defendant's
15 possession was adequately secured and protected.
16

17 108. Defendant also had a duty to exercise appropriate clearinghouse practices to
18 remove from an Internet-accessible environment the PII it was no longer required to retain
19 pursuant to regulations and had no reasonable need to maintain in an Internet-accessible
20 environment.

21 109. Defendant also had a duty to have procedures in place to detect and prevent the
22 improper access and misuse of the PII of Plaintiffs and the Class.

23 110. Defendant's duty to use reasonable security measures arose as a result of the
24 special relationship that existed between Defendant and Plaintiffs and the Classes. That special
25 relationship arose because Defendant acquired Plaintiffs and the Classes' confidential PII in the
26 course of its business practices.
27

28 111. Defendant was subject to an "independent duty," untethered to any contract

1 between Defendant and Plaintiffs or the Class.

2 112. A breach of security, unauthorized access, and resulting injury to Plaintiffs and
3 the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security
4 practices.

5 113. Plaintiffs and the Class were the foreseeable and probable victims of any
6 inadequate security practices and procedures. Defendant knew or should have known of the
7 inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of
8 providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's
9 systems.
10

11 114. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the
12 Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and
13 opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included
14 its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and
15 the Class, including basic encryption techniques freely available to Defendant.
16

17 115. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly
18 remains in, Defendant's possession.

19 116. Defendant was in a position to protect against the harm suffered by Plaintiffs and
20 the Classes as a result of the Data Breach.

21 117. Defendant had and continues to have a duty to adequately disclose that the PII of
22 Plaintiffs and the Class within Defendant's possession might have been compromised, how it was
23 compromised, and precisely the types of data that were compromised and when. Such notice was
24 necessary to allow Plaintiffs and the Classes to (i) take steps to prevent, mitigate, and repair any
25 identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and
26 detrimental use of their sensitive information.
27

28 118. Defendant had a duty to employ proper procedures to prevent the unauthorized

1 dissemination of the PII of Plaintiffs and the Class.

2 119. Defendant has admitted that the PII of Plaintiffs and the Class were wrongfully
3 lost and disclosed to unauthorized third persons as a result of the Data Breach.

4 120. Defendant, through its actions and/or omissions, unlawfully breached its duties to
5 Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in
6 protecting and safeguarding the PII of Plaintiffs and the Class during the time the PII was within
7 Defendant's possession or control.

8 121. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the
9 Class in deviation of standard industry rules, regulations, and practices at the time of the Data
10 Breach.

11 122. Defendant failed to heed industry warnings and alerts to provide adequate
12 safeguards to protect the PII of Plaintiffs and the Classes in the face of increased risk of theft.

13 123. Defendant, through its actions and/or omissions, unlawfully breached its duty to
14 Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent
15 dissemination of the PII.

16 124. Defendant breached its duty to exercise appropriate clearinghouse practices by
17 failing to remove from the Internet-accessible environment any PII it was no longer required to
18 retain pursuant to regulations and which Defendant had no reasonable need to maintain in an
19 Internet-accessible environment.

20 125. Defendant, through its actions and/or omissions, unlawfully breached its duty to
21 adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data
22 Breach.

23 126. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs
24 and the Class, the PII of Plaintiffs and the Class would not have been compromised.

25 127. There is a close causal connection between Defendant's failure to implement
26
27
28

1 security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent
2 harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class were lost and
3 accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding
4 such PII by adopting, implementing, and maintaining appropriate security measures.

5
6 128. As a direct and proximate result of Defendant's negligence, Plaintiffs and the
7 Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii)
8 the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft
9 of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery
10 from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs
11 associated with effort expended and the loss of productivity addressing and attempting to mitigate
12 the actual and future consequences of the Data Breach, including but not limited to efforts spent
13 researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs
14 associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain
15 in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant
16 fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Class;
17 and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect,
18 contest, and repair the impact of the PII compromised as a result of the Data Breach for the
19 remainder of the lives of Plaintiffs and the Class.
20

21
22 129. As a direct and proximate result of Defendant's negligence, Plaintiffs and the
23 Class have suffered and will continue to suffer other forms of injury and/or harm, including, but
24 not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic
25 losses.

26 130. Additionally, as a direct and proximate result of Defendant's negligence,
27 Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII,
28 which remain in Defendant's possession and is subject to further unauthorized disclosures so long

as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

131. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Classes are entitled to recover actual, consequential, and nominal damage.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Classes)

132. Plaintiffs and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein. This claim is pled in the alternative to the breach of express contract claim and all the other claims herein.

133. Plaintiffs bring this claim individually and on behalf of the Class.

134. When Plaintiffs and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII, comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII, and to timely notify them in the event of a data breach.

135. Defendant solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendant's provision of financial services. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

136. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

137. Plaintiffs and Class Members paid money to Defendant to receive financial services. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

138. Plaintiffs and Class Members would not have provided their PII to Defendant had

1 they known that Defendant would not safeguard their PII, as promised, or provide timely notice of
2 a data breach.

3 139. Plaintiffs and Class Members fully performed their obligations under their
4 implied contracts with Defendant.

5 140. Defendant breached its implied contracts with Plaintiffs and Class Members by
6 failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely
7 and accurate notice of the Data Breach.

8 141. The losses and damages Plaintiffs and Class Members sustained, include, but are
9 not limited to:

10
11 a. Theft of their PII;

12 b. Costs associated with purchasing credit monitoring and identity theft
13 protection services;

14 c. Costs associated with the detection and prevention of identity theft and
15 unauthorized use of their PII;

16 d. Lowered credit scores resulting from credit inquiries following fraudulent
17 activities;

18 e. Costs associated with time spent and the loss of productivity from taking
19 time to address and attempt to ameliorate, mitigate, and deal with the actual and future
20 consequences of the Data Breach – including finding fraudulent charges, cancelling and
21 reissuing cards, enrolling in credit monitoring and identity theft protection services,
22 freezing and unfreezing accounts, and imposing withdrawal and purchase limits on
23 compromised accounts;

24 f. The imminent and certainly impending injury flowing from the increased
25 risk of potential fraud and identity theft posed by their PII being placed in the hands of
26 criminals;
27
28

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

142. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff sand the Classes)

143. Plaintiffs and the Class reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

144. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' contractual based claims pursuant to Fed. R. Civ. P. 8.

145. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII.

146. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant

1 instead elected to increase its own profits at the expense of Plaintiffs and Class Members by
2 utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand,
3 suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over
4 the requisite security.

5
6 147. Under the principles of equity and good conscience, Defendant should not be
7 permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant
8 failed to implement appropriate data management and security measures that are mandated by its
9 common law and statutory duties.

10 148. Defendant failed to secure Plaintiffs and Class Members' PII and, therefore, did
11 not provide full compensation for the benefit Plaintiffs and Class Members provided.

12 149. Defendant acquired the PII through inequitable means in that it failed to disclose
13 the inadequate security practices previously alleged.

14
15 150. If Plaintiffs and Class Members knew that Defendant had not reasonably secured
16 their PII, they would not have agreed to provide their PII to Defendant.

17 151. Plaintiffs and Class Members have no adequate remedy at law.

18 152. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class
19 Members have suffered and will continue to suffer other forms of injury and/or harm.

20 153. Defendant should be compelled to disgorge into a common fund or constructive
21 trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.
22 In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class
23 Members overpaid for Defendant's services.

24
25 **PRAYER FOR RELIEF**

26
27 **WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, request judgment
28 against Defendant and that the Court grant the following:

- 1 A. For an Order certifying the Nationwide Class and appointing Plaintiffs and their
2 Counsel to represent such Classes;
- 3 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
4 complained of herein pertaining to the misuse and/or disclosure of the PII of
5 Plaintiffs and Class Members, and from refusing to issue prompt, complete, any
6 accurate disclosures to Plaintiffs and Class Members;
- 7
8 C. For injunctive relief requested by Plaintiffs, including but not limited to,
9 injunctive and other equitable relief as is necessary to protect the interests of
10 Plaintiffs and Class Members, including but not limited to an order:
- 11 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
12 described herein;
- 13 ii. requiring Defendant to protect, including through encryption, all data
14 collected through the course of its business in accordance with all applicable
15 regulations, industry standards, and federal, state or local laws;
- 16 iii. requiring Defendant to delete, destroy, and purge the personal identifying
17 information of Plaintiffs and Class Members unless Defendant can provide to the
18 Court reasonable justification for the retention and use of such information when
19 weighed against the privacy interests of Plaintiffs and Class Members;
- 20 iv. requiring Defendant to implement and maintain a comprehensive Information
21 Security Program designed to protect the confidentiality and integrity of the PII of
22 Plaintiffs and Class Members;
- 23 v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class
24 Members on a cloud-based database;
- 25 vi. requiring Defendant to engage independent third-party security
26 auditors/penetration testers as well as internal security personnel to conduct testing,
27
28

- 1 including simulated attacks, penetration tests, and audits on Defendant's systems
2 on a periodic basis, and ordering Defendant to promptly correct any problems or
3 issues detected by such third-party security auditors;
- 4 vii. requiring Defendant to engage independent third-party security auditors and
5 internal personnel to run automated security monitoring;
- 6 viii. requiring Defendant to audit, test, and train its security personnel regarding
7 any new or modified procedures;
- 8 ix. requiring Defendant to segment data by, among other things, creating
9 firewalls and access controls so that if one area of Defendant's network is
10 compromised, hackers cannot gain access to other portions of Defendant's systems;
- 11 x. requiring Defendant to conduct regular database scanning and securing
12 checks;
- 13 xi. requiring Defendant to establish an information security training program that
14 includes at least annual information security training for all employees, with
15 additional training to be provided as appropriate based upon the employees'
16 respective responsibilities with handling personal identifying information, as well
17 as protecting the personal identifying information of Plaintiffs and Class Members;
- 18 xii. requiring Defendant to routinely and continually conduct internal training and
19 education, and on an annual basis to inform internal security personnel how to
20 identify and contain a breach when it occurs and what to do in response to a breach;
- 21 xiii. requiring Defendant to implement a system of tests to assess its respective
22 employees' knowledge of the education programs discussed in the preceding
23 subparagraphs, as well as randomly and periodically testing employees compliance
24 with Defendant's policies, programs, and systems for protecting personal
25 identifying information;
- 26
27
28

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: September 16, 2024

Respectfully submitted,

/s/ Ryan Samano

Alex J. De Castroverde

Nevada Bar No. 6950

Ryan Samano

Nevada Bar No. 15995

DE CASTROVERDE LAW GROUP

1149 S. Maryland Pkwy

Las Vegas, NV 89104

Phone: (702) 222-9999

Fax: (702) 383-8741

Ryan@dlgteam.com

/s/ Leigh S. Montgomery

Leigh S. Montgomery

(pro hac vice forthcoming)

Texas Bar No. 24052214

EKSM, LLP

1105 Milford Street

Houston, Texas 77006

Phone: (888) 350-3931

Fax: (888) 276-3455

lmontgomery@eksm.com

*Counsel for Plaintiffs and the Proposed
Class*